



AnexSPOT: Give your Customers Access to the Internet Simply and with Complete Security

Hotels, cafes, bars, etc are faced with an increasing demand for guest and visitor connectivity throughout the entire premises; guest rooms, restaurants, lobbies, outdoor areas. Having the ability to offer an internet access service will provide the opportunity to increase the visitors by offering free access or secure on-going revenue for the business, increase the company profile and win new customers and provide a valuable service to customers and guests. AnexSPOT client-server is a complete authentication, authorization and accounting server. AnexSPOT provides an array of rich features ensuring property owners get revenue stream and guests get good Internet experience. AnexSPOT is mainly aimed at the hospitality segment and organizations intending to implement Wi-Fi network access at their premises.

Key Benefits:

- Secure hot spot support: AnexSPOT can be used to create guest access networks by setting up hot-spot networks. Administrators can easily require web-based user authentication or terms-of-use approval prior to providing network access. This enables convenient, yet controlled access for guest users, without compromising corporate revenues.
- Secure wireless connectivity Support: AnexSPOT supports Wi-Fi access point (802.11b/g/n) supporting multiple security protocols. **Support for LDAP, Radius, the standard protocol for managing remote authentication**
- **Integrated SQL database that avoids the need to install additional software**
- Easy management: One time only setup and installation fee or small monthly fee with no initial hardware costs. Organizations can set different tariff rates for visitors, or retain all revenue from users. They can offer customizable "Home page" for advertising their business.
- Internet usage can be easily charged by pre-defined billing plans (by minute, hour, day or other options).
- AnexSPOT offers homepage redirection as well as multiple URL-link redirections for advertising options for service providers, hotels or property owners. The appliance allows service providers or system administrators to create a 'walled garden' where unauthenticated users can be granted free access to selected links.

AnexSPOT: A Complete Security Solution:

AnexSPOT is fully integrated with **AnexGATE UTM**, India's leading network security Appliance . This means **complete security for you and your customers** against Internet threats, such as viruses, unauthorized connections, and access to illegal or unwanted content.

This unique characteristic makes AnexSPOT a top level solution for:

- Offering your customers a completely secure connection service
- Boosting the quality and value of your offer
- Creating new business opportunities and increasing your profits

Whether you are running a private activity (such as a hotel, a café or a restaurant) or you are working in the public sector (such as in libraries, schools, universities, airports), and you want to offer a simple and secure connection to the Internet, AnexSPOT is the solution for you.

**AnexSPOT
Range of Products**

AnexSPOT 50(AS50)
AnexSPOT 100(AS100)
AnexSPOT 200+(AS200+)

Technical features for server:

Platform: Rack Mount 1 U platform
 Processor: Mid to High-End Processor
 Memory: Upto 2 GB RAM (depend on model)
 HDD: 250 GB
 Interfaces: Giga Interface
 Power: AC 100 – 240 VAC (50/60Hz)
 Color: Red



Specifications

Firewall		Networking /Routing	
Stateful Packet Filter Firewall	Yes	Static routes	Yes
Network attack detection	Yes	Source-based routing	Yes
IP & Mac Address based policy	Yes	Policy-based routing	Yes
DoS and DDoS protection	Yes	Equal-Cost Multipath (ECMP)	Yes
TCP reassembly for fragmented packet protection	Yes	Dynamic Routing * RIP (V1/V2)	Yes
Brute force attack mitigation	Yes	Multicast	Yes
SYN cookie protection	Yes	Reverse Path Forwarding (RPF)	Yes
Zone-based IP spoofing	Yes	Internet Group Management Protocol (IGMP) (v1, v2)	Yes
Malformed packet protection	Yes	IGMP Proxy	Yes
Unified Threat Management		PIM single mode	Yes
IPS (Deep Inspection firewall)	Yes	PIM source-specific multicast	Yes
Protocol anomaly detection	Yes	Multicast inside IPSec tunnel	Yes
Stateful protocol signatures	Yes	IP Address Assignment	
IPS/DI attack pattern obfuscation	Yes	Static	Yes
Gateway Antivirus	Yes	DHCP, PPPoE client	Yes
Instant message AV	Yes	Internal DHCP server	Yes
Signature database	Yes	Multi-WAN with Failover & Load Balance	
Protocols scanned	Yes	Support for multiple Uplinks/WANs	Yes
Anti-spyware	Yes	Automatic WAN Uplink Failover & Load balancing	Yes
Anti-adware	Yes	USB Data /3G support	Yes
Anti-keylogger	Yes	Monitoring of WAN Uplinks	Yes
Anti-spam	Yes	Uplink types: Ethernet (Static/DHCP), PPPoE, ADSL,Data Card	Yes
Integrated URL filtering	Yes	DDNS	Yes
Web Security		Administration, Logging/Monitoring	
Application proxy	Yes	Admin and Read Only user levels	Yes
Transparent Proxy support	Yes	Software/Patch upgrades	Yes
URL Filtering	Yes	Configuration Backup & Rollback	Yes
Authentication: Inter. Database, LDAP, Active Directory	Yes	Syslog (multiple servers)	Yes
Group Based web Access Policies	Yes	Notification through SMS* & Email	Yes
Time Based Access control with multi-Time intervals	Yes	SNMP (v2)/Inventory management (add-ons)	Yes
User /Group identity Based Bandwidth Management	Yes	IPTraf / TCP Dump	Yes
Download & Upload Limit Control	Yes	Graphical Bandwidth report	Yes
User Authentication and Access Control		Graphical browsing usage report	Yes
Built-in (internal) database - user limit	Yes	Security Reports for Suspicious Activities	Yes
Third-party user authentication	Yes	Attack Logs & logging of Intrusions	Yes
RADIUS accounting	Yes	Remote Management	Yes
Web-based authentication	Yes	NetIQ Web Trends	Yes
Unified access control (UAC) enforcement point	Yes	SNMP (v2)	Yes
VPN		SNMP full custom MIB	Yes
Secure SSL/IPSec/PPTP	Yes	Traceroute	Yes
Advanced Encryption Standard (AES) (256-bit)	Yes	VPN tunnel monitor	Yes
Encryption 3DES, RC4, SHA-1, MD-5, ESP, AH	Yes	WiFi and internet links uptime/downtime monitoring and reports	Yes
Manual key, Internet Key Exchange (IKE) Public key infrastructure	Yes	System Management	
Perfect forward secrecy (DH Groups)	Yes	Web UI (HTTP and HTTPS)	Yes
Prevent replay attack	Yes	Command line interface (console)	Yes
Remote access VPN	Yes	Command line interface (telnet)	Yes
IPSec Network Address Translation (NAT) traversal	Yes	Command line interface (SSH)	Yes
True SSL/TLS VPN	Yes	All management via VPN tunnel on any interface	Yes
Manual key, Internet Key Exchange (IKE) Public key infrastructure	Yes	rapid deployment	Yes
Hotspot		Wireless security	
Captive portal	Yes	Wireless privacy	WPA, WPA2(AES or TKIP),IPsec VPN, WEP
Wired/wireless support	Yes	Wireless authentication	PSK, EAP-PEAP, EAP-TLS, EAP-TTLS over 802.1x
Pre/post-paid and free tickets	Yes	MAC access controls	Permit or deny
Integrated WPA/RADIUS based authentication and accounting and browser/OS based authentication	Yes	Client isolation	Yes
Connection logging	Yes		
No additional software/hardware required	Yes		
Per-user and global bandwidth limiting	Yes		
MAC-address based user accounts	Yes		
User accounts import/export per CSV	Yes		
Single-click ticket generation (Easy Ticket)	Yes		

* All specifications and photos are subject to change without notice

For More Details Contact:

Smile Security and Surveillance Pvt. Ltd.

#21/2, MRI Building, First Floor, 14KM, Old Madras Road, Bhattarahalli, K.R Puram, Bangalore -560 049. (INDIA)

Tel : +91- 80- 25614 773/774/775/776 Fax: +91- 80- 25614666

Email: info@sssl.co.in Website: www.sssl.co.in